Universidade de Brasília Faculdade UnB Gama

Criptografia e Segurança de Redes
Trabalho 3

Alunos: Matrículas:
João Paulo Nunes Soares 15/0038267
Josué Nascimento da Silva 15/0038933

- INSTRUÇÕES DE USO
  - **Exercício 1**
    - Para compilar o arquivo execute na pasta do arquivo: **gcc exe1.c -o main .**
    - Para executar o programa execute: **./main**
    - Ao executar o programa, insira primeiro a chave de até 256 bytes, e depois a quantidade de bytes que se deseja gerar.
      - OBS: A saída estará em um arquivo presente no mesmo local do executável com o nome **saida.dat** , escrita no formato binário para execução na suíte de testes.
      - OBS 2: Alguns análises gerados pela suit de testes em arquivos gerados por este exercício estão na pasta teste/ dentro do diretório deste exercício.Ambos foram gerados com <stream length> igual a 1000000 com uma execução de 10 bitstreams, e ambos os arquivos possuiam 5000000 bytes.
  - **Exercício 2**
    - Para compilar o arquivo execute na pasta do arquivo: **gcc exe2.c -lm -o testeMiller** .
    - Para executar o programa execute: **./testeMiller**
    - Após executar,escolha um numero impar para conferir se é primo e em seguida a quantidade de teste a serem feitas.

- LIMITAÇÕES CONHECIDAS
  - **Exercício 1**
    - Não há limitações conhecidas.
  - **Exercício 2**
    - Devem ser inseridos apenas numeros inteiro que possam ser expressos dentro de uma variavel do tipo “int”
    - O intervalo para o valor da quantidade de testes deve ser de [2 , n-2] , onde n é o valor para conferir se é primo ou não

- DIVISÃO DO TRABALHO

- ✔ Ambos os alunos realizaram a atividade, onde a maior parte foi realizada no modelo de pareamento.